A User Anonymous Mutual Authentication Protocol

Saru Kumari[1], Xiong Li[2, 3], Fan Wu[4], Ashok Kumar Das[5], Vanga Odelu[6], Muhammad Khurram Khan7

[1]Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India
[e-mail: saryusiirohi@gmail.com]
[2]School of Computer Science and Engineering, Hunan University of Science and Technology
Xiangtan 411201, China
[e-mail: lixiong84@gmail.com]
[3]School of Computer and Software, Nanjing University of Information Science and Technology,
Nanjing 210044, China
[4]Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China
[5]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology
Hyderabad 500032, India
[6] Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur 721302, India
[7]Centre of Excellence in Information Assurance (CoEIA), King Saud University
Riyadh, Kingdom of Saudi Arabia
*Corresponding author: Xiong Li

Received April 24, 2016; revised July 6, 2016; accepted July 20, 2016;
published September 30, 2016

Abstract

Widespread use of wireless networks has drawn attention to ascertain confidential communication and proper authentication of an entity before granting access to services over insecure channels. Recently, Truong et al. proposed a modified dynamic ID-based authentication scheme which they claimed to resist smart-card-theft attack. Nevertheless, we find that their scheme is prone to smart-card-theft attack contrary to the author's claim. Besides, anyone can impersonate the user as well as service provider server and can breach the confidentiality of communication by merely eavesdropping the login request and server's reply message from the network. We also notice that the scheme does not impart user anonymity and forward secrecy. Therefore, we present another authentication scheme keeping apart the threats encountered in the design of Truong et al.'s scheme. We also prove the security of the proposed scheme with the help of widespread BAN (Burrows, Abadi and Needham) Logic.

Keywords: Guessing and Impersonation attacks, Authentication, Forward secrecy, BAN Logic.

This research was supported by National Natural Science Foundation of China (No. 61300220, No. 61572013, No. 61572188), and it is also supported by PAPD, CICAEET. Fan Wu was supported by University Distinguished Young Research Talent Training Program of Fujian Province 2016 and the Education Scientific Research Project for Young Teachers of Fujian (No. JA14369). Muhammad Khurram Khan thanks to the support of the Deanship of Scientific Research at King Saud University for itsfunding this Prolific Research Group (PRG-1436-16).

http://dx.doi.org/10.3837/tiis.2016.09.026 **ISSN : 1976-7277**

1. Introduction

Now-a-days, various services and an intended communication with some distant entity is just a click away due to fast growing technological advancement. It has created tremendous opportunities in the market and imparted a great deal of convenience to the users. However, this entire Internet based set-up demands for proper security, confidentiality and authenticity to provide transparency and avoid deceit in transactions carried over insecure network. To achieve such goals, many encryption schemes [1-4] have been proposed. Remote user authentication schemes are capable to fulfill this demand efficiently due to provisions like user authentication, mutual authentication and confidential communication between the participants.

The origin of user authentication schemes goes back to 1981 when Lamport [5] proposed a method for password authentication with insecure network. Subsequently, many password-based authentication schemes [6-13] were presented. However, most of these schemes deployed the static identity of the user. In practice, static identity is not preferable in many scenarios such as financial matters and applications requiring high level security also need that user be kept anonymous. This gave invent to the concept of dynamic identity by Das [14] in terms of a user authentication scheme based on the concept of dynamic identity. Das's scheme attracted many researchers [15-20] to analyze the new proposal. In 2012, Chen et al. [21] presented a password authentication scheme, they claimed it to withstand lost smart card attack and provide mutual authentication. However, we observe a number of attacks in their scheme such as insider, impersonation, DoS and password guessing attack. Besides, it still suffers from lost smart card attack and lack of user anonymity, confidential communication, forward secrecy and other important characteristics. In 2012, Lee [20] observed that Das's scheme is susceptible to impersonation and guessing attacks. Lee also proposed a scheme to resist these attacks. Recently, Wen et al. [22] and Truong et al. [23] independently highlighted some security problems on Lee's scheme in view of the researches by Kocher et al. [24] and Messerges et al. [25] over the security of smart cards. They showed that in Lee's scheme, a legal user of the system can impersonate the other users as well as the server without knowing the information stored in user's smart card; and anyone can guess user's password by extracting the secrets stored in user's smart card. Truong et al. also revealed that Lee's scheme achieves only one way authentication at the server side and cannot establish the session key essential for confidential communication. Therefore, Truong et al. presented an improved version [23] of Lee's scheme [20].

1.1 Threat Model

Throughout this paper, we abide by the following threat model. An adversary can extract from smart card the information stored in it by analyzing its power consumption report. An adversary is capable of eavesdropping the communications carried between the user and the server over public channel and can alter or resend these messages. But an adversary cannot guess the password and identity concurrently in real polynomial time.

1.2 Our contribution

In this paper, we study Truong et al.'s user authentication scheme based on the concept of dynamic identity, analyze the extent to which it maintains the merits and improves the weaknesses of Lee's scheme, identify its demerits, and finally put forward a scheme with better performance. We observe that Truong et al.'s scheme preserves the advantages of Lee's scheme, like resistance to replay and stolen verifier attacks, and provision of freely password update facility to its users. We find that Truong et al.'s scheme extends the unilateral authentication to mutual authentication by adding three-way challenge response mechanism, adds the feature of session key, offers efficient login and password change phase by incorporating a verification mechanism in smart card, and mended the privileged insider attack. Thus, Truong et al.'s scheme improves Lee's scheme as just mentioned. However, we find that Truong et al.'s scheme fails to justify authors' assertion that their scheme is secure under smart-card-theft situation since the situation leads to the guessing of user's password. Besides, their scheme is weak to resist the impersonation attacks and cannot provide confidential communication. In fact, an adversary can not only masquerade as a registered user and the authorized server but can also read the confidential communication by computing the agreed session key. Consequently, mutual authentication fails even after employing three-way challenge response mechanism and user anonymity is not achieved though the smart card computes different identity for each session. Therefore, at many places Truong et al.'s scheme falls short to improve Lee's scheme. Further, the established session key in their scheme does not provide forward secrecy. Hence, we find enough scope of improvement in Truong et al.'s scheme. Eventually, we propose an authentication scheme keeping the merits and enhancing the security aspects of Truong et al.'s scheme. We make use of the elliptic curve cryptography (ECC) [26-27] to provide forward secrecy and try our best to overcome the aforementioned security weaknesses.

1.3 Organization of the remaining paper

Section 2 gives reviewof scheme by Truong et al. and Section 3 is about its cryptanalysis. Section 4, deals with preliminaries necessary useful in this paper and also presents the proposed scheme. Sections 5 & 6 pertain to conventional and BAN-logical security analysis respectively, of our scheme. Section 7 & 8 are for comparision and conclusion.

2. Review of Truong et al.'s Scheme

Here follows Table 1for notations useful for this paper:

Table 1. The notations and their meaning

Notations	Description
S	Remote Server
U	A registered user
E	An adversary
ID_i, PW_i & SC	Identity, password & smart card of U
x	Secret key of S
r_i/e_i	Nonce chosen by user/server during registration process
R_i/R_s	Nonce chosen by user/server during login-authentication process
$SessK$	Session-key
p,n	Large prime numbers
F_p	A finite field of prime order p
$E_p(a,b)$	An elliptic curve defined over F_p
P	A point of $E_p(a,b)$ called the base point, P is of order n
Θ	The infinity point
$\oplus$	Exclusive-OR operator
$h(.)$	A one-way hash function
$\|\|$	Concatenation operator

A detailed description of Truong et al.'s scheme is as follows:

2.1 Registration Phase

This phase is about the registration of U with S, for which the following steps are executed by both the entities:

1) U chooses her/his identity ID_i, a password PW_i, a random number r_i and computes $h(PW_i\| r_i)$.
2) Submits $\{ID_i, h(PW_i\| r_i)\}$ to S securely.

On receiving $\{ID_i, h(PW_i\| r_i)\}$ as the registration request, from U, S does the following tasks:

3) Generates e_i, a random value, and computes $A_i = h[ID_i\|h(PW_i\|r_i)]\oplus h(x\|e_i)$, $L_i= h[ID_i\|h(PW_i\|r_i) \|h(x \|e_i)]$.
4) Issues SC to U containing $\{A_i, L_i, e_i, h(.)\}$ through a secure channel.

On receiving SC, U does the following:

5) Inserts r_i into SC so that $SC =\{A_i, L_i, e_i, r_i, h(\cdot)\}$.

2.2 Login Phase

This phase is conducted over a public channel. For the purpose of login and obtaining services from S, U computes her/his login request as follows:

1) Inserts SC into the card-reader and then keys in ID_i and PW_i.
2) SC obtains $h(x \|e_i) = A_i\oplus h(ID_i\|h(PW_i\|r_i))$ and checks if L_i is equal to $h[ID_i\| h(PW_i\| r_i) \| h(x \| e_i)]$ computed. For correct match, SC proceeds; otherwise, disrupts the session.
3) Generates R_i, a nonce, and computes $CID_i = ID_i\oplus R_i$, $B_i = h(x \|e_i) \oplus R_i$ and $C_i = h[ID_i\|R_i\| h(x \| e_i)]$.
4) Transmits $\{CID_i, B_i, C_i, e_i\}$ to S.

2.3 Mutual Authentication & Session Key Agreement Phase

This phase is conducted over a public channel. First of all S performs the following after receiving $\{CID_i, B_i, C_i, e_i\}$ from U:

1) Obtains $R_i^*=B_i\oplus h(x\|e_i)$, $ID_i= CID_i\oplus R_i^*$and checks the validity of ID_i. For valid ID_i, S proceeds; otherwise, declines the login request.
2) Checks if C_i is equal to $h[ID_i\|R_i^*\|h(x\|e_i)]$. For correct match, S proceeds; otherwise, disrupts the session.
3) Generates R_s, a nonce, and computes $K_s= h(ID_i\|R_i^*) \oplus R_s$, $V_s= h[R_s\|h(x\|e_i)]$. Then S transmits $\{K_s, V_s\}$ to U.

On receiving $\{K_s, V_s\}$ from S, U performs the following tasks:

4) Computes $R_s^*= K_s\oplus h(ID_i\|R_i)$ and checks if$V_s$is equal to $h(R_s^*\|h(x\|e_i))$. For correct match, S is authenticated successfully; otherwise, U disrupts the session.
5) Computes $M_i= h(R_i\|R_s)$ and transmits M_i to S.

On receiving M_i from U, S performs the following tasks:

6) Checks if M_i is equal to $h(R_i^*\|R_s)$. For correct match, U is authenticated successfully; otherwise, S disrupts the session.
7) If the mutual authentication is successfully achieved, S computes $SessK= h(R_i^*\|h(x\|e_i)\|R_s)$ and U computes $SessK = h(R_i\|h(x\|e_i)\|R_s^*)$.

2.4 Password Update Phase

This phase is to facilitate the user to update his password at its will for which U executes the following steps:

1) Inserts SC into the card-reader, keys in ID_i, PW_i and her/his newly chosen password PW_{inew}.
2) SC obtains $h(x \| e_i) = A_i \oplus h(ID_i \| h(PW_i \| r_i))$ and checks if L_i is equal to $h[ID_i \| h(PW_i \| r_i) \| h(x \| e_i)]$ computed. For correct match, SC proceeds; otherwise, disrupts the session.
3) Computes $A_{inew} = h(x \| e_i) \oplus h[ID_i \| h(PW_{inew} \| r_i)]$, $L_{inew} = h[ID_i \| h(PW_{inew} \| r_i) \| h(x \| e_i)]$ and finally replaces A_i with A_{inew} and L_i with L_{inew}.

3. Cryptanalysis of Truong et al.'s Scheme

Since the login and mutual authentication & key agreement phase take place on the public channel, therefore, messages transmitted in these phases are available for interception by an adversary E. Moreover, the information stored in user's smart card can be retrieved [24, 25]. Besides, the secret key of user/server may leak. In the light of the aforementioned scenario, we present the security problems of Truong et al.'s scheme.

3.1 Security Breaches through Login Request Interception

We reveal that Truong et al.'s scheme is frail in case E intercepts the login request of any user. The listing and the discussion of various security problems of Truong et al.'s scheme are given below:

- Lack of user anonymity (Identity guessing is possible) [28-31]
- User/server impersonation attack [29-35]
- Attack on confidential communication [29-36]
- Password guessing attack via smart card loss/theft [29, 31, 33-36]
- Lacks forward secrecy [29, 31, 37]

Identity guessing attack: Suppose an adversary E intercepts the login request $\{CID_i, B_i, C_i, e_i\}$ of U. Then he efforts to reveal the identity of the user. E guesses ID_i^* and computes $R_i^* = CID_i \oplus ID_i^*$, $(h(x \| e_i))^* = B_i \oplus R_i^*$ and $C_i^* = h[ID_i^* \| R_i^* \| (h(x \| e_i))^*]$. Checks if C_i is equal to C_i^*, if not then E repeats the procedure with another guess for user's identity. However, the correct match yields the correct identity ID_i along with correct nonce R_i and the secret $h(x \| e_i)$. Thus, user anonymity is not provided by the scheme. This defect is due to the violation of the public-key principle proposed in [38]: under the non-tamper-resistance assumption of smart cards, no scheme can achieve user anonymity without employing public-key techniques.

User impersonation attack: As discussed above, an adversary E can possess ID_i and $h(x \| e_i)$ of U by intercepting $\{CID_i, B_i, C_i, e_i\}$ of U. Then E is capable of impersonating U at any time as described below:
1) Generates a nonce R_E and computes $CID_E = ID_i \oplus R_E$, $B_E = h(x \| e_i) \oplus R_E$ and $C_E = h[ID_i \| R_E \| h(x \| e_i)]$.
2) Transmits $\{CID_E, B_E, C_E, e_i\}$ to S.

On obtaining the login request $\{CID_E, B_E, C_E, e_i\}$, S performs the following tasks:
3) Obtains $R_E^* = B_E \oplus h(x \| e_i)$, $ID_i = CID_E \oplus R_E^*$ and checks the validity of ID_i. Clearly, ID_i would be valid as it is the actual dentity of U who is the registered user. So, S accepts the login request.
4) Checks if C_E is equal to $h[ID_i \| R_E^* \| h(x \| e_i)]$. Clearly, the two values would match and S will proceed further.
5) Generates a nonce R_s and computes $K_s = h(ID_i \| R_E^*) \oplus R_s$, $V_s = h[R_s \| h(x \| e_i)]$. Then S transmits $\{K_s, V_s\}$ to U.

On receiving $\{K_s, V_s\}$ from S, E performs the following tasks:
6) E computes $R_s^* = K_s \oplus h(ID_i \| R_E)$ and can check if V_s is equal to $h(R_s^* \| h(x \| e_i))$ to validate S.
7) Computes $M_E = h(R_E \| R_s^*)$ and transmits M_E to S.
On receiving M_E, S performs the following tasks:
8) Checks if M_E is equal to $h(R_E^* \| R_s)$ which would obviously match. So, S believes that U is authenticated successfully and hence E is granted access to U's account.

Server impersonation attack: An adversary E possessing ID_i, $h(x \| e_i)$ and e_i of U can easily recognize the login request $\{CID_i, B_i, C_i, e_i\}$ of U due to the presence of e_i. E can cheat U by masquerading as S in the following way:

1) E blocks the login request $\{CID_i, B_i, C_i, e_i\}$ from reaching to S.
2) Obtains $R_i^* = B_i \oplus h(x \| e_i)$, generates a nonce $R_E$and computes $K_E = h(ID_i \| R_i^*) \oplus R_E$, $V_E = h[R_E \| h(x \| e_i)]$. Then E transmits $\{K_E, V_E\}$ to U.
On receiving $\{K_E, V_E\}$, U performs the following tasks:
3) Obtains $R_E^* = K_E \oplus h(ID_i \| R_i)$ and checks if V_E is equal to $h(R_E^* \| h(x \| e_i))$ which would obviously be correct. So, U believes that the origin of the message $\{K_E, V_E\}$ is from S and feels to be connected with the legal server.

Attack on confidential communication: The adversary E having ID_i, $h(x \| e_i)$ and e_i corresponding to the user U can intercept messages $\{CID_i, B_i, C_i, e_i\}$ and $\{K_s, V_s\}$ from the open network. Then E can recover R_i and R_s by computing $R_i = B_i \oplus h(x \| e_i)$ and $R_s = K_s \oplus h(ID_i \| R_i)$ respectively. Further, E is able to compute $SessK = h(R_i \| h(x \| e_i) \| R_s)$ established between U and S. Consequently, E can read the confidential messages exchanged between U and S.

Password guessing attack via smart card loss/theft: An adversary E can maintain a record of the intercepted login requests of many users. If E steals/finds the lost smart card of some user, suppose$U$, then he can extract [24-25] the values $\{A_i, L_i, e_i, r_i, h(.)\}$ stored in it. E can easily match this smart card with the corresponding login request $\{CID_i, B_i, C_i, e_i\}$ from the record due to the presence of the common value e_i. Then E can obtain the identity ID_i and secret $h(x \| e_i)$ of U by applying identity guessing attack as explained earlier. Now E can proceed to guess the password of U in the following way. E guesses PW_i^* as U's password and computes $L_i^* = h[ID_i \| h(PW_i^* \| r_i) \| h(x \| e_i)]$. If E finds $L_i^* = L_i$, it implies that the guess PW_i^* is correct; or else he repeats the process with some other guess. In this way, the scheme fails to resist the smart card theft attack. For a comprehensive taxonomy of smart-card-loss-based password guessing attacks, readers are referred to [39].

3.2 Lack of Forward Secrecy

An authentication scheme satisfies the forward secrecy when the security of the session keys established in previous sessions is not affected due to revelation of the secret keys of the participant entities (server's secret key/user's password). In case the secret key x of S is disclosed, E can intercept the login request $\{CID_i, B_i, C_i, e_i\}$ and response message $\{K_s, V_s\}$ related to a user, suppose U. Then E can easily compute $h(x \| e_i)$ and hence can obtain $R_i = B_i \oplus h(x \| e_i)$, $ID_i = CID_i \oplus R_i$ and $R_s = K_s \oplus h(ID_i \| R_i)$. Finally, E computes the session key $SessK = h(R_i \| h(x \| e_i) \| R_s)$ which is to be established between U and S. In the same way, E can reveal the previously established session keys using already intercepted pair of login request and response message. Thus, forward secrecy is not available in the scheme.

4. The Proposed Scheme

Before presenting our scheme, we give a concise information about an elliptic curve along with its computational problems [26-27] and an important remark related to the proposed scheme.

Preliminary: Elliptic Curve Cryptography **(ECC):** In (ECC), the elliptic curve equation is given by $E_p(a, b) : y^2 = x^3 + ax + b \pmod p$ over a finite field F_p of prime order $p > 3$, where, a, $b \in F_p$ and $4a^3 + 27b^2 \neq 0 \pmod p$. For an integer $r \in F_p^*$ and a point $P \in E_p(a, b)$, the elliptic curve point multiplication $r \cdot P$ over $E_p(a, b)$ is defined as $r \cdot P = P + P + \ldots + P$ (r times). Here follow two intractable problems:

- **Elliptic Curve Discrete Logarithm Problem (ECDLP)**: Given two points P & Q belonging to $E_p(a, b)$, this problem asks to find another integer $r \in F_p^*$ where $Q = r \cdot P$.
- **Elliptic Curve Diffie-Hellman Problem (ECDHP)**: Given three points P, $r \cdot P$, $s \cdot P$ belonging to $E_p(a, b)$ for $r, s \in F_p^*$, this problem asks to find the point $r \cdot s \cdot P$ over $E_p(a, b)$.

Now, we present our scheme in which security troubles discussed in previous Section have no existance. Summary of the proposed scheme is in **Fig. 1**.

Remark 1: Suppose we want to apply bitwise XOR between two numbers of diverse lengths. This can be done as per the details in [40]. First pad the smaller number with leading zeros to make its length equal to the length of the larger number. Afterwards, we can bitwise XOR the two numbers. For instance, let x and y be two numbers of 128-bit and 64-bit length respectively. First pad y with leading 64 zeros so that the resulting number is of 128-bit length. Now, x and y can be XORed bitwise to give an outcome of 128-bit length. In this way, two numbers of diverse lengths can be XORed bitwise [40-41].

4.1 Initial phase

S selects a large prime number p and the base point $P \in E_p$ with very large prime order n, i.e., $n \cdot P = \Theta$ and $P \neq \Theta$. S also selects a cryptographic one-way hash function $h(.)$ and makes $\{E_p, P, F_p\}$ public.

4.2 Registration Phase

This phase is about the registration of U with S, for which both the entities perform the steps as given below:

1) U chooses her/his identity ID_i, a password PW_i, a random number r_i and computes $h(PW_i \| r_i)$.
2) Submits $\{ID_i, h(PW_i \| r_i)\}$ to S securely.
3) Generates a random value e_i and computes $A_i = h[ID_i \| h(PW_i \| r_i)] \oplus h(x \| e_i)$, $L_i = h[ID_i \| h(PW_i \| r_i) \| h(x \| e_i)]$ and $Q_i = h[h(PW_i \| r_i) \| ID_i] \oplus e_i$.
4) Issues U a smart card SC containing $\{A_i, L_i, Q_i, h(.)\}$ through a secure channel.

On receiving SC, U does the following:

5) Inserts $P_i = h(ID_i \| PW_i) \oplus r_i$ into SC so that $SC = \{A_i, L_i, Q_i, P_i, h(.)\}$.

4.3 Login Phase

This phase is conducted over a public channel. To login S to obtain services, U computes her/his login request:

1) First inserts SC into the card reader then inputs ID_i and PW_i.

2) *SC* obtains $r_i = P_i \oplus h(ID_i \,\|\, PW_i)$, $h(x \,\|\, e_i) = A_i \oplus h(ID_i \,\|\, h(PW_i \,\|\, r_i))$ and checks if L_i is equal to $h[ID_i \,\|\, h(PW_i \,\|\, r_i) \,\|\, h(x \,\|\, e_i)]$ computed. For correct match, *SC* proceeds; otherwise, disrupts the session.
3) Obtains $e_i = Q_i \oplus h[h(PW_i \,\|\, r_i) \,\|\, ID_i]$ and generates a nonce R_i. Then computes $CID_i = h[h(x \,\|\, e_i)] \oplus (ID_i \,\|\, R_i \cdot P)$, and $C_i = h[ID_i \,\|\, h(x \,\|\, e_i) \,\|\, R_i \cdot P]$.
4) Transmits $\{CID_i, C_i, e_i\}$ to S.

User (*U*)		**Server (*S*)**
Registration Phase:		Generates random e_i
Chooses ID_i, PW_i&r_i	$\xrightarrow{\{ID_i,\ h(PW_i\| r_i)\}}$	$A_i= h[ID_i\| h(PW_i\| r_i)] \oplus h(x \,\|\, e_i)$
Computes $h(PW_i\| r_i)$		$L_i= h[ID_i\| h(PW_i\| r_i) \,\|\, h(x \,\|\, e_i)]$ and
	$\xleftarrow{SC_i= \{A_i,\ L_i,\ Q_i,\ h(.)\}}$	$Q_i= h[h(PW_i\| r_i)\| ID_i] \oplus e_i$
Insert $P_i= h(ID_i\| PW_i) \oplus r_i$ into SC_i		
$SC_i= \{A_i, L_i, Q_i, P_i, h(.)\}$		

User (*U*)		**Server (*S*)**
***Login and Mutual Authentication and Session Key Agreement Phase*:**		
U: Inserts ID_i, PW_i		
SC: $r_i \leftarrow P_i \oplus h(ID_i\| PW_i)$		
$h(x \,\|\, e_i) \leftarrow A_i \oplus h(ID_i\| h(PW_i\| r_i))$		
For$L_i= h[ID_i\| h(PW_i\| r_i) \,\|\, h(x \,\|\, e_i)]$		
$e_i \leftarrow Q_i \oplus h[h(PW_i\| r_i)\| ID_i]$		
$CID_i= h[h(x \,\|\, e_i)] \oplus (ID_i\|R_i\cdot P)$		
$C_i= h[ID_i\| h(x \,\|\, e_i) \,\|\, R_i\cdot P]$		
	$\xrightarrow{\{CID_i,\ C_i,\ e_i\}}$	$[ID_i^*\|(R_i\cdot P)^*] \leftarrow CID_i \oplus h[h(x \,\|\, e_i)]$
		For $C_i= h[ID_i^*\| \ h(x \,\|\, e_i) \,\|\, (R_i\cdot P)^*]$
	$\xleftarrow{\{R_s\cdot P,\ V_s\}}$	$V_s= h[R_s\cdot P \,\|\, h(x \,\|\, e_i) \,\|\, (R_i\cdot P)^* \,\|\, ID_i^*]$
For $V_s= h[R_s\cdot P \,\|\, h(x \,\|\, e_i) \,\|(R_i\cdot P)\| ID_i]$		
$SessK= h[R_i\cdot (R_s\cdot P)\| h(x \,\|\, e_i) \,\|\, ID_i]$		
$M_i= h[SessK\| h(x \,\|\, e_i) \,\|\, ID_i]$	$\xrightarrow{\{M_i\ \}}$	$SessK= h[R_s\cdot (R_i\cdot P)^*\| h(x \,\|\, e_i) \,\|\, ID_i^*]$
		For $M_i= h[SessK\| h(x \,\|\, e_i) \,\|\, ID_i^*]$
		U is authenticated

User (*U*)		**Smart Card (*SC*)**
Password Change Phase:		
U: Inserts ID_i, PW_i, PW_{inew}	$\xrightarrow{\{ID_i,\ PW_i,\ PW_{inew}\}}$	$r_i \leftarrow P_i \oplus h(ID_i\| PW_i)$
		$h(x \,\|\, e_i) \leftarrow A_i \oplus h(ID_i\| h(PW_i\| r_i))$
		For $L_i= h[ID_i\| h(PW_i\| r_i) \,\|\, h(x \,\|\, e_i)]$
		$e_i \leftarrow Q_i \oplus h[h(PW_i\| r_i)\| ID_i]$
		$A_{inew}= h(x \,\|\, e_i) \oplus h[ID_i\| h(PW_{inew}\| r_i)]$
		$L_{inew}= h[ID_i\| h(PW_{inew}\| r_i) \,\|\, h(x \,\|\, e_i)]$
		$Q_{inew}= h[h(PW_{inew}\| r_i)\| ID_i] \oplus e_i$
		$P_{inew}= h(ID_i\| PW_{inew}) \oplus r_i$
		$A_{inew} \leftarrow A_i$, $L_{inew} \leftarrow L_i$,$Q_{inew} \leftarrow Q_i$and $P_{inew} \leftarrow P_i$

Fig. 1. The Proposed Scheme

4.4 Mutual Authentication & Session Key Agreement Phase

This phase is conducted over a public channel. It is about achieving mutual authentication and session key agreement between U and S. First of all, S executes the following steps after receiving $\{CID_i, C_i, e_i\}$ from U:

1) Retrieves $[ID_i^* \,||\, (R_i\cdot P)^*] = CID_i \oplus h[h(x \,||\, e_i)]$ and checks if C_i is equal to $h[ID_i^* \,||\, h(x \,||\, e_i) \,||\, (R_i\cdot P)^*]$. For correct match, the validity of U's identity is proved and S proceeds; otherwise, declines the login request.
2) Generates a nonce R_s and computes $R_s\cdot P$ & $V_s = h[R_s\cdot P \,||\, h(x \,||\, e_i) \,||\, (R_i\cdot P)^* \,||\, ID_i^*]$. Then S transmits $\{R_s\cdot P, V_s\}$ to U.

On receiving $\{R_s\cdot P, V_s\}$ from S, U performs the following tasks:

3) Checks if V_s is equal to $h[R_s\cdot P \,||\, h(x \,||\, e_i) \,||\, (R_i\cdot P) \,||\, ID_i]$. For correct match, S is authenticated successfully; otherwise, U disrupts the session.
4) Computes $SessK = h[R_i \cdot (R_s\cdot P) \,||\, h(x \,||\, e_i) \,||\, ID_i]$, $M_i = h[SessK \,||\, h(x \,||\, e_i) \,||\, ID_i]$ and transmits M_i to S.

On receiving M_i from U, S performs the following tasks:

5) Computes $SessK = h[R_s \cdot (R_i\cdot P)^* \,||\, h(x \,||\, e_i) \,||\, ID_i^*]$ and checks if M_i is equal to $h[SessK \,||\, h(x \,||\, e_i) \,||\, ID_i^*]$. For correct match, U is authenticated successfully and S grants U access to the service(s) for which U is entitled; otherwise, S disrupts the session.

4.5 Password Update Phase

This phase is to facilitate the user to update her/his password at its will for which U executes the following steps:

1) First inserts SC into the card reader then inputs ID_i, PW_i and a newly chosen password PW_{inew}.
2) SC obtains $r_i = P_i \oplus h(ID_i \,||\, PW_i)$, $h(x \,||\, e_i) = A_i \oplus h(ID_i \,||\, h(PW_i \,||\, r_i))$ and checks if L_i is equal to $h[ID_i \,||\, h(PW_i \,||\, r_i) \,||\, h(x \,||\, e_i)]$ computed. For correct match, SC proceeds; otherwise, disrupts the session.
3) Obtains $e_i = Q_i \oplus h[h(PW_i \,||\, r_i) \,||\, ID_i]$. Computes $A_{inew} = h(x \,||\, e_i) \oplus h[ID_i \,||\, h(PW_{inew} \,||\, r_i)]$, $L_{inew} = h[ID_i \,||\, h(PW_{inew} \,||\, r_i) \,||\, h(x \,||\, e_i)]$, $Q_{inew} = h[h(PW_{inew} \,||\, r_i) \,||\, ID_i] \oplus e_i$ and $P_{inew} = h(ID_i \,||\, PW_{inew}) \oplus r_i$.
4) Finally, replaces A_i with A_{inew}, L_i with L_{inew}, Q_i with Q_{inew} and P_i with P_{inew}.

5. Security Analysis of the Proposed Scheme

This section measures the strength of our scheme in the scenario for which Truong et al.'s scheme is shown vulnerable. First of all, we show the key improvements done in our scheme over Truongs' scheme. Then we discuss the Security features of our scheme in detail. Further, we highlight the features which the proposed scheme inherits from Truong et al.'s scheme.

5.1 Key Improvements in Our Scheme over Truongs' Scheme

- In U's smart card, the random nonce e_i is not stored in plaintext. It is stored under protection of U's ID_i and PW_i as $Q_i = h[h(PW_i \,||\, r_i) \,||\, ID_i] \oplus e_i$. Thus, an adversary, who happens to obtain the smart card of a user, cannot obtain e_i unless he knows ID_i and PW_i of U. So the adversary cannot misuse random nonce e_i.
- However, e_i is available in plaintext in login request but an adversary has no way how to match login message and smart card of a specific user. This is due to unavailability of any

common value in both login message and smart card.

- Our scheme is communication cost efficient as its login message contains only three parameters while login message of Troung et al.'s scheme contains four parameters.
- To protect U's identity, in login phase, the message transmitted is $\{CID_i, C_i, e_i\}$ in which $CID_i = h[h(x \parallel e_i)] \oplus (ID_i \parallel R_i \cdot P)$ is changed from $CID_i = ID_i \oplus R_i$ used in Troung et al.'s scheme. Here we have used the goodness of elliptic curve cryptography to protect the user's identity. This restricts the activity of identity guessing.
- Once an adversary has no access to user's identity, he cannot mount impersonation attacks, other guessing (password) attacks, confidentiality breach, and other attacks dependent on knowing the ID_i of U_i. This is an important feature of our scheme.
- In our scheme, the session key $SessK = h[R_i \cdot (R_s \cdot P) \parallel h(x \parallel e_i) \parallel ID_i]$ established between the user and the server possesses forward secrecy property which is indispensable for security. A session key without forward secrecy property cannot efficiently fulfill the purpose of confidential communication.

5.2 Security Features of the Proposed Scheme

5.2.1 Provision of User Anonymity

E can intercept the login request $\{CID_i, C_i, e_i\}$ of U. But to guess the identity ID_i of U using $CID_i = h[h(x \parallel e_i)] \oplus (ID_i \parallel R_i \cdot P)$ and C_i, he needs $R_i \cdot P$ which is not available. Further, E cannot verify the guessed value of U's identity since CID_i involves $h[h(x \parallel e_i)]$ whereas $C_i = h[ID_i \parallel h(x \parallel e_i) \parallel R_i \cdot P]$ involves $h(x \parallel e_i)$. It is not feasible to obtain $h(x \parallel e_i)$ from $h[h(x \parallel e_i)]$ due to one-way property of hash functions. Further, since ID_i is protected by one-way hash function in user's SC, so E cannot recover U's ID_i even if he obtains U's SC and extracts the information stored in it. Moreover, SC and the login request of U do not contain any identical value using which these two can be matched and prove helpful to trace the user's identity. Thus, the user anonymity is provided by the proposed scheme.

5.2.2 Resistance to Impersonation Attacks

To impersonate U, E should possesses U's identity ID_i and the shared secret $h(x \parallel e_i)$. Although, every login request $\{CID_i, C_i, e_i\}$ of U contains the random number e_i in plaintext but without knowing the secret key x of the server, E cannot compute $h(x \parallel e_i)$. It is not possible to obtain $h(x \parallel e_i)$ or ID_i from $C_i = h[ID_i \parallel h(x \parallel e_i) \parallel R_i \cdot P]$ due to one-way property of hash functions. Further, E cannot recover U's identity ID_i as mentioned in subsection 5.2.1. For similar reason, E cannot cheat U by masquerading as S. Without having $h(x \parallel e_i)$, E cannot recover ID_i and $R_i \cdot P$ from $CID_i = h[h(x \parallel e_i)] \oplus (ID_i \parallel R_i \cdot P)$. Hence E cannot compute justifiable V_s to send a valid response message corresponding to an intercepted and blocked login request of U. So, the scheme resists user (server) impersonation attacks.

5.2.3 Provision of Confidential Communication

In order to compute $SessK = h[R_i \cdot (R_s \cdot P) \parallel h(x \parallel e_i) \parallel ID_i] = h[R_s \cdot (R_i \cdot P)^* \parallel h(x \parallel e_i) \parallel ID_i^*]$, an adversary E must possess the following values: ID_i, $h(x \parallel e_i)$, R_i, R_s & $(R_i \cdot P)$. It is clear from the previous subsections that E has no way to obtain ID_i or/and $h(x \parallel e_i)$. Besides, E cannot gain $R_i \cdot P$ from $CID_i = h[h(x \parallel e_i)] \oplus (ID_i \parallel R_i \cdot P)$ by intercepting a login request unless he possess the correct $h(x \parallel e_i)$. Although, $R_s \cdot P$ is available in plaintext through S's response message $\{R_s \cdot P, V_s\}$ travelling over the public channel, E cannot find R_s from $R_s \cdot P$ owing to ECDLP. Further, it is not feasible to recover $SessK$ from $M_i = h[SessK \parallel h(x \parallel e_i) \parallel ID_i]$ traversing the public channel due to one-way property of hash function [42-43]. Hence, the proposed scheme ensures confidential communication.

5.2.4 Resistance to Smart Card Loss /Password Guessing Attack

Consider the situation when E finds the lost SC of U and extracts [24-25] the information $\{A_i, L_i, Q_i, P_i, h(.)\}$ stored in it. But U's password is protected by the one-way property of hash function in each of A_i, L_i, Q_i and P_i. To correctly guess and verify PW_i, E requires the knowledge of ID_i, r_i, and $h(x \| e_i)$. Further, the random number r_i is not stored in plaintext in SC so E is not at ease to guess PW_E and compute $h(PW_E \| r_i)$ in order to identify U's password. To get r_i from P_i, E should know U's ID_i as well as PW_i. For similar reasons, E cannot obtain U's identity ID_i or secret value $h(x \| e_i)$ from SC. Further, it is not possible to guess U's password from an intercepted login request $\{CID_i, C_i, e_i\}$ as all its constituent values are independent of PW_i. A lost or stolen SC of U is not useful for guessing PW_i or gaining any other value of interest.

5.2.5 Provision of Perfect Forward Secrecy

Assuming the situation of the disclosure of S's secret key x, E can intercept the login request $\{CID_i, C_i, e_i\}$ of U and can easily compute $h(x \| e_i)$. But, to compute an agreed session key $SessK = h[R_i \cdot (R_s \cdot P) \| h(x \| e_i) \| ID_i]$, the adversary E also needs ID_i, R_i, R_s & $(R_i \cdot P)$. However, E has no way to obtain ID_i as explained in subsection 5.2.1. Besides, E cannot gain $R_i \cdot P$ from $CID_i = h[h(x \| e_i)] \oplus (ID_i \| R_i \cdot P)$ by intercepting a login request unless he possess ID_i. Although, E can get $R_s \cdot P$ from the network, E cannot obtain R_s from $R_s \cdot P$ due to ECDLP. Alternately, if U's password PW_i as well as identity ID_i are disclosed then E requires the corresponding SC. By extracting P_i and A_i from SC, E can obtain r_i and $h(x \| e_i)$ by computing $r_i = P_i \oplus h(ID_i \| PW_i)$ and $h(x \| e_i) = A_i \oplus h[ID_i \| h(PW_i \| r_i)]$ respectively. E can get CID_i from the network and can also gain $R_i \cdot P$ as $(ID_i \| R_i \cdot P) = CID_i \oplus h[h(x \| e_i)]$. But, E still cannot compute $SessK$ in the absence of R_s. Thus, even after possessing SC, ID_i and PW_i, the adversary cannot compute the established $SessK$. Hence, the scheme provides perfect forward secrecy.

5.2.6 Provides Mutual Authentication

S verifies the legitimacy of U in two stages: firstly by verifying the equivalence $C_i = h[ID_i^* \| h(x \| e_i) \| (R_i \cdot P)^*]$ and secondly by verifying the equivalence $M_i = h[SessK \| h(x \| e_i) \| ID_i^*]$. U verifies the legitimacy of S by checking the equivalence $V_s = h[R_s \cdot P \| h(x \| e_i) \| (R_i \cdot P) \| ID_i]$. In addition to hold or retrieve the values ID_i or $h(x \| e_i)$, E should also possess $R_i \cdot P$ & R_i in order to compute a valid reply message $\{R_s \cdot P, V_s = h[R_s \cdot P \| h(x \| e_i) \| (R_i \cdot P)^* \| ID_i^*]\}$ like S and a valid challenge response $M_i = h[SessK \| h(x \| e_i) \| ID_i]$ with $SessK = h[R_i \cdot (R_s \cdot P) \| h(x \| e_i) \| ID_i]$ like U. But only U knows the value $R_i \cdot P$ and only S can retrieve it from $CID_i = h[h(x \| e_i)] \oplus (ID_i \| R_i \cdot P)$ received in a login request. Moreover, no one can obtain R_i from $R_i \cdot P$ due to ECDLP. As a result, no one except the valid user and the valid server can prove its legitimacy else it is detectable and results in disruption of the session. Furthermore, no one can impersonate any legal participant of the scheme (as discussed in subsection 5.2.2) and the established session key ensures confidential communication (as discussed in subsection 5.2.3 and 5.2.5). Thus, our scheme offers proper mutual authentication.

5.2.7 Merits Inherited from Truong et al.'s Scheme

- ***Resistance to replay attack:*** Use of nonce R_i & R_s and three-way challenge response mechanism imparts resistance to replay attack. E can replay the login request $\{CID_i, C_i, e_i\}$ but due to lack of $h(x \| e_i)$ and ID_i he cannot compute a valid response M_i. Further, if E replays $\{R_s \cdot P, V_s\}$ then U would disrupt the session as the replayed V_s would not pass the verification test since random numbers used in each session are different. Thus, replay of any message is useless.
- ***Resistance to stolen verifier attack:*** Since S does not keep any tabular record of user specific values (user's identity, password, etc), therefore, no question arises of such an attack.
- ***Provides session key:*** U and S compute a common session key $h[R_i \cdot (R_s \cdot P) \| h(x \| e_i) \| ID_i] = SessK = h[R_s \cdot (R_i \cdot P)^* \| h(x \| e_i) \| ID_i^*]$ to communicate confidentiality after mutual authentication.
- ***Resistance to known key attack:*** On compromise of $SessK = h[R_i \cdot (R_s \cdot P) \| h(x \| e_i) \| ID_i]$ of a particular session, E can neither obtain $h(x \| e_i)$ nor R_i & R_s because of the one-way property of hash function. Along with $h(x \| e_i)$, the $SessK$ is also based on nonce R_i & R_s which differ from one session to another; and it is not possible to predict nonce to be used in any future session. Hence, E gets no information about a future session key. Therefore, the design of $SessK$ is safe from the known key attack.
- ***Resistance to session-specific temporary attack:*** In case, the session specific random numbers R_i & R_s are disclosed, E still cannot compute the session key $SessK = h[R_i \cdot (R_s \cdot P) \| h(x \| e_i) \| ID_i]$ in the want of $h(x \| e_i)$ and ID_i. Thus, our scheme is not vulnerable to session-specific temporary attack introduced in [44].
- ***Provides freely password changing facility:*** U can freely change her/his password without any interaction with S.
- ***Provides efficient login and password change phase:*** Whenever U wishes to login S or wants to change her/his password, every time smart card checks the correctness of the entered ID_i and PW_i by means of the equivalence $L_i = h[ID_i \| h(PW_i \| r_i) \| h(x \| e_i)]$. Therefore, it is not feasible for E to login S with wrong identifiers or to update user's SC with an arbitrary password.
- ***Resistance to Denial of service attack:*** A user itself cannot login with wrong identifiers due to correctness verification mechanism $L_i = h[ID_i \| h(PW_i \| r_i) \| h(x \| e_i)]$ in SC, so he cannot face denial of service due to her/his own mistake [45]. Moreover, E cannot cause U to face the denial of service by accessing and manipulating the records maintained by S since the server does not keep any record of user specific values.
- ***Resistance to privileged insider attack:*** In the registration phase, U submits $h(PW_i \| r_i)$ which protects her/his password from guessing and hence our scheme resists privileged insider attack.

6. Security Proof of the Proposed Scheme using BAN-Logic

We conduct the security analysis of our proposed scheme using Burrows-Abadi-Needham Logic (BAN-logic) [46]. We show that the scheme allows a user to establish a session key with the server near the end of the authentication process. Let $U$and S be the user, and the server respectively. The three elementary items of BAN-logic are statements/formulas, principals and encryption keys. Let Y & X are symbols for statements, Q & P are symbols for principals, and K is symbol for cryptographic encryption key. Basic logic notations of BAN-logic needed to analyze our scheme is given below:

- $P \mid\equiv X$: P believes X.
- $P \lhd X$: P sees/receives X.
- $P \mid\sim X$: P once said X (or P sent X).
- $P \mid\Rightarrow X$: P controls X.
- $\#(X)$: X is fresh.
- $P \overset{K}{\leftrightarrow} Q$: P and Q communicate using shared key K.
- (X): The hashed value of X.
- $(X, Y)_K$: Take hash of X and Y using K as key.
- $\langle X, Y\rangle_Y$: Combine X and Y using Y.
- $SessK$: Session key for current authentication session

Some basic BAN-logic postulates are as mentioned below:

- Message meaning rule:
  $\dfrac{PbelievesP\overset{K}{\leftrightarrow}Q,\ \ Psees\{X\}_K}{PbelievesQsaidX}$ or $\dfrac{P|\equiv P\overset{K}{\leftrightarrow}Q,\ \ P\lhd\{X\}_K}{P|\equiv Q|\sim X}$
- Nonce-verification rule:
  $\dfrac{Pbelieves\text{ fresh }X,\ \ PbelievesQsaidX}{PbelievesQbelievesX}$ or $\dfrac{P|\equiv \#(X),\ \ P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$
- Jurisdiction rule:
  $\dfrac{PbelievesQcontrolsX,\ \ PbelievesQbelievesX}{PbelievesX}$ or $\dfrac{P|\equiv P|\Longrightarrow X,\ \ P|\equiv Q|\equiv X}{P|\equiv X}$
- Freshness rule:
  $\dfrac{Pbelieves\text{ fresh }X}{Pbelieves\text{ fresh }(X{,}Y)}$ or $\dfrac{P|\equiv \#(X)}{P|\equiv \#(X{,}Y)}$
- Believe rule:
  $\dfrac{PbelievesQbelieves(X{,}Y)}{PbelievesQbelievesX}$ or $\dfrac{P|\equiv Q|\equiv(X{,}Y)}{P|\equiv Q|\equiv X}$, $\dfrac{PbelievesX,\ \ PbelievesY}{Pbelieves\ (X{,}Y)}$ or $\dfrac{P|\equiv X,\ \ P|\equiv Y}{P|\equiv\ (X{,}Y)}$

The proposed scheme should satisfy the following goals:

- $Goal_1{:}U|\equiv (U \overset{SessK}{\longleftrightarrow} S)$
- $Goal_2{:}U|\equiv S|\equiv (U \overset{SessK}{\longleftrightarrow} S)$
- $Goal_3{:}S|\equiv (U \overset{SessK}{\longleftrightarrow} S)$
- $Goal_4{:}S|\equiv U|\equiv (U \overset{SessK}{\longleftrightarrow} S)$

The scheme in idealized form in terms of the messages exchanged is given below:

- Message$_1$: $U \rightarrow S$: $\langle ID_i, \left(U \overset{ID_i}{\leftrightarrow} S\right), R_i \cdot P, \left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right)\rangle_{h(x||e)}$
- Message$_2$: $S \rightarrow U$: $\left(ID_i, R_i \cdot P, R_s \cdot P, \left(U \overset{R_s \cdot P}{\longleftrightarrow} S\right)\right)_{h(x||e)}$

- Message$_3$: $U \rightarrow S$: $\left(ID_i,, h(x||e), \left(U \overset{SessK}{\longleftrightarrow} S\right)\right)_{SessK}$

Here, we make initial state assumptions pertaining to the scheme:

- $\mathcal{A}_1$: $U|\equiv (U \overset{ID_i}{\leftrightarrow} S)$
- $\mathcal{A}_2$:$U|\equiv (U \overset{h(x||e)}{\longleftrightarrow} S)$
- $\mathcal{A}_3$:$S| \equiv (U \overset{h(x||e)}{\longleftrightarrow} S)$
- $\mathcal{A}_4$: $S|\equiv \# (R_i \cdot P)$
- $\mathcal{A}_5$: $U|\equiv \# (R_s \cdot P)$
- $\mathcal{A}_6$: $S|\equiv U|\Rightarrow (U \overset{ID_i}{\leftrightarrow} S)$
- $\mathcal{A}_7$: $S|\equiv U|\Rightarrow (U \overset{R_i \cdot P}{\longleftrightarrow} S)$
- $\mathcal{A}_8$: $U| \equiv S| \Rightarrow (U \overset{R_s \cdot P}{\longleftrightarrow} S)$

Now, we will utilize BAN-logic postulates and rules to show that U&S successfully share a common session key *SessK* to ensure confidential communication.

- From Message$_1$, we have
$$S \lhd \langle ID_i, \left(U \overset{ID_i}{\leftrightarrow} S\right), R_i \cdot P, \left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right)\rangle_{h(x||e)} \tag{1}$$
- From (1), $\mathcal{A}_3$and the message meaning rule, we get
$$S|\equiv U|\sim \langle ID_i, \left(U \overset{ID_i}{\leftrightarrow} S\right), R_i \cdot P, \left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right)\rangle \tag{2}$$
- From $\mathcal{A}_4$and the freshness-conjuncatenation rule, we obtain
$$S|\equiv \# \langle ID_i, \left(U \overset{ID_i}{\leftrightarrow} S\right), R_i \cdot P, \left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right)\rangle \tag{3}$$
- From (2), (3) and the nonce-verification rule, we deduce
$$S|\equiv U|\equiv \langle ID_i, \left(U \overset{ID_i}{\leftrightarrow} S\right), R_i \cdot P, \left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right)\rangle \tag{4}$$
- From (4) and believe rule, we infer
$$S|\equiv U|\equiv \left(U \overset{ID_i}{\leftrightarrow} S\right)\text{and} \tag{5}$$
$$S|\equiv U|\equiv \left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right) \tag{6}$$
- From $\mathcal{A}_6$, (5) and jurisdiction rule, we have
$$S|\equiv\left(U \overset{ID_i}{\leftrightarrow} S\right) \tag{7}$$
- From $\mathcal{A}_7$, (6) and jurisdiction rule, we have
$$S|\equiv\left(U \overset{R_i \cdot P}{\longleftrightarrow} S\right) \tag{8}$$
- From Message$_2$, we have
$$U \lhd \left(ID_i, R_i \cdot P, R_s \cdot P, \left(\overset{R_s \cdot P}{\longleftrightarrow} S\right)\right)_{h(x||e)} \tag{9}$$
- From (9), $\mathcal{A}_2$and the message meaning rule, we obtain
$$U|\equiv S|\sim \left(ID_i, R_i \cdot P, R_s \cdot P, \left(U \overset{R_s \cdot P}{\longleftrightarrow} S\right)\right) \tag{10}$$
- From $\mathcal{A}_5$,and the freshness-conjuncatenation rule, we infer

$$U|\equiv \#\left(ID_i, R_i \cdot P, R_s \cdot P, \left(U \overset{R_s\cdot P}{\longleftrightarrow} S\right)\right) \quad (11)$$

- From (10), (11) and the nonce-verification rule, we deduce

$$U|\equiv S|\equiv \left(ID_i, R_i \cdot P, R_s \cdot P, \left(U \overset{R_s\cdot P}{\longleftrightarrow} S\right)\right) \quad (12)$$

- From (12) and believe rule, we get

$$U|\equiv S|\equiv \left(U \overset{SessK}{\longleftrightarrow} S\right) \quad Goal2$$

- From $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_8$, *goal*$_2$and the jurisdiction rule, we obtain

$$U|\equiv\left(U \overset{SessK}{\longleftrightarrow} S\right) \quad Goal1$$

- From Message$_3$, we have

$$S \triangleleft \left(ID_i,, h(x||e), \left(U \overset{SessK}{\longleftrightarrow} S\right)\right)_{SessK} \quad (13)$$

- From (13), $\mathcal{A}_3$and the message meaning rule, we infer

$$S|\equiv U|\sim \left(ID_i,, h(x||e), \left(U \overset{SessK}{\longleftrightarrow} S\right)\right) \quad (14)$$

- From (7), (8),$\mathcal{A}_4$and the freshness-conjuncatenation rule, we deduce

$$S|\equiv \#\left(ID_i,, h(x||e), \left(U \overset{SessK}{\longleftrightarrow} S\right)\right) \quad (15)$$

- From (14), (15) and the nonce-verification rule, we obtain

$$S|\equiv U|\equiv \left(ID_i,, h(x||e), \left(U \overset{SessK}{\longleftrightarrow} S\right)\right) \quad (16)$$

- From (16) and the believe rule, we get

$$S|\equiv U|\equiv (U \overset{SessK}{\longleftrightarrow} S) \quad Goal4$$

- From (7), $\mathcal{A}_7$, *Goal*$_4$ and the jurisdiction rule, we obtain

$$S|\equiv(U \overset{SessK}{\longleftrightarrow} S) \quad Goal3$$

According to *Goal*1, *Goal*2, *Goal*3and *Goal*4, we conclude that $U(S)$ have trust that $S(U)$ believes that the session key *SessK* between them is shared successfully.

7. Comparative Performance Analysis of the Proposed Scheme

This section analyzes the performance of the proposed scheme by comparing it with Truong et al.'s [23], Chen et al.'s [21] and Lee's scheme [20].We present the comparative analysis at three levels:

- Comparison of memory capacity and communication cost (**Table 2**)
- Comparison of computational complexity (**Table 3**)
- Comparison of security features (**Table 4**)

For the first two levels, we assume that the random numbers {r_i, e_i, etc}, the outcome of an elliptic curve point multiplication {R_s· P, R_s · (R_i· P), etc}, the outcome of exponential operation, the output of modular multiplication/division operation, and the output of one-way hash function {C_i, V_s, M_i, etc} are of 160 bits. It is clear from **Table 2** that in our scheme *SC* does not require additional space in memory and the cost for communication is 160 bits lesser than needed in Truong et al's and Chen et al.'s schemes. Thus, our scheme excels in performance at the first level.

Table 2. Comparison of memory capacity and communication cost

Schemes→ ↓Memory Capacity & Communication Cost	Lee's [20]	Chen et al.'s [21]	Truong et al.'s [23]	Our Scheme
Memory space required by *SC*	2*160 = 320 bits	4*160 = 640 bits	4*160 = 640 bits	4*160 = 640 bits
Communication cost	3*160 = 480 bits	7*160 = 1120 bits	7*160 = 1120 bits	6*160 = 960 bits

Table 3. Comparison of computational complexity

Schemes→ ↓Phases	Lee's [20]	Chen et al.'s [21]	Truong et al.'s [23]	Our Scheme
Registration phase(*U/SC*)	Nil	Nil	$1t_h$	$2t_h$
Registration phase(*S*)	$1t_h$	$1t_h+1t_e$	$3t_h$	$4t_h$
Login-authentication phase(*U/SC*)	$4t_h$	$3t_h+2t_m+2t_e$	$8t_h$	$9t_h+2t_{epm}$
Login-authentication phase(*S*)	$3t_h$	$2t_h+1t_m+1t_e$	$6t_h$	$6t_h+2t_{epm}$
Aggregate computational complexity	$8t_h$	$6t_h+3t_m+4t_e$	$18t_h$	$21t_h+4t_{epm}$

t_h is the time complexity for computing one-way hash operation; t_{epm} is the time complexity for computing elliptic curve point multiplication; $t_e$is the time complexity of exponential operation; t_m is the time complexity of multiplication/division operation.

To compare the computational complexity, we neglect the lightweight operations like exclusive-OR operation and string concatenation. **Table 3** depicts the increment of one hash operation at the user side during registration phase from nil computational load in Lee's and Chen et al.'s schemes to Truong et al.'s and our scheme. During the same phase, *S* operates only one hash function more than Truong et al.'s scheme whereas in Truong et al.'s scheme *S* operates two hash functions more than Lee's scheme. Unlike Chen et al.'s scheme, our scheme is free from costly modular exponential function. At the user side during login-authentication phase, Truong et al.'s scheme uses four more hash operations than Lee's scheme whereas our scheme uses one hash function and two elliptic curve point multiplication operations more than Truong et al.'s scheme. In the same phase, *S* operates only two elliptic curve point multiplication operations more than Truong et al.'s scheme and requires no additional hash operations. Only Chen et al.'s scheme uses multiplication/division operation and the time consuming exponential operation. If we look at the aggregate computational load, Truong et al.'s scheme uses ten more hash operations than Lee's scheme whereas our scheme requires three hash operations and four elliptic curve point multiplication operations more than Truong et al.'s scheme. Although hash overhead is lowest in Chen et al.'s scheme, it is not lightweight due to the involvement of four exponential operations. Undoubtedly, the computational complexity of our scheme is more than that of schemes in [20, 21, 23] but it boosts the security to a considerable extent as is apparent from **Table 4** and discussed below.

Although Truong et al.'s scheme improves upon insider attack applicable on Lee's and Chen et al.'s schemes but stores the random numbers r_i and e_i directly in *SC* which leaves their scheme [23] vulnerable to smart card loss attack and allows an adversary to match a *SC* with the corresponding login request. Chen et al.'s scheme is also susceptible to smart card loss attack. Our scheme not only resists to insider attack but is also free from weaknesses just mentioned about Truong et al.'s and Chen et al.'s schemes. Truong et al.'s scheme falls short to remedy impersonation attacks and fulfill the requirement of confidential communication of Lee's and Chen et al.'s schemes. Further, Truong et al.'s scheme is susceptible to password guessing attack via smart card loss as in Lee's scheme; this attack is also applicable on Chen et al.'s scheme. Our scheme not only amends these security problems of Truong et al.'s and Chen et al.'s schemes but also retains all their merits as depicted in **Table 4**. Although our scheme employs complex elliptic curve point multiplication operation, it provides perfect forward secrecy which is an important ingredient of the security of the session key. It is noticeable that Chen et al.'s scheme fails to offer forward secrecy property though it uses complex exponential operation. In the absence of the forward secrecy, the established session key cannot guarantee the confidentiality of communication between the user and the server.

Table 4. Comparison of Security Features

Schemes→ ↓Security Threats	Lee's [20]	Chen et al.'s [21]	Truong et al.'s [23]	Our Scheme
Provides user anonymity	No	No	No	Yes
Resistance to impersonation attacks	No	No	No	Yes
Ensures confidential communication	No	No	No	Yes
Resist smart card loss attack	No	No	No	Yes
Resists password guessing attack	No	No	No	Yes
Provides perfect forward secrecy	N/A	No	No	Yes
Provides mutual authentication	No	No	No	Yes
Resists replay attack	Yes	Yes	Yes	Yes
Resists stolen verifier attack	Yes	Yes	Yes	Yes
Resists known key attack	N/A	Yes	Yes	Yes
Resists session-specific temporary attack	N/A	Yes	Yes	Yes
Provides freely password changing facility	Yes	No	Yes	Yes
Provides efficient login & password updation	No	No	Yes	Yes
Resists denial of service attack	No	No	Yes	Yes
Resists insider attack	No	No	Yes	Yes

N/A means not applicable

8. Conclusion

This paper is about the study of a newly proposed dynamic ID-based authentication scheme, and remedying its weaknesses. Our review has revealed that the scheme given by Truong et al. cannot withstand smart-card-theft attack as this situation facilitates the guessing of user's password. We have also shown that their scheme fails to provide mutual authentication since an adversary can cheat any of the legal participant through impersonation. Further, it is showed that the established session key is inefficient to fulfill the purpose of confidential communication due to lack of forward secrecy and defies the aim of dynamic identity. In order to remove these drawbacks we have presented a scheme with refined security. We have shown the excellence of our scheme over the related schemes through security analysis and comparison.

References

[1] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340-352, 2015. Article (CrossRef Link)

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, “Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement,” *IEEE Transactions on Parallel and Distributed Systems*, 2015. Article (CrossRef Link)

[3] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, “Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing,” *IEICE Transactions on Communications*, vol. E98-B, no. 1, pp.190-200, 2015. Article (CrossRef Link)

[4] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, “Mutual Verifiable Provable Data Auditing in Public Cloud Storage,” *Journal of Internet Technology*, vol. 16, no. 2, pp. 317-323, 2015. Article (CrossRef Link)

[5] L. Lamport, “Password authentication with insecure communication,” *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981. Article (CrossRef Link)

[6] G. Horng, “Password authentication without using password table,” *Information Processing Letters*, vol. 55, pp. 247-250, 1995. Article (CrossRef Link)

[7] J.K. Jan, and Y.Y. Chen, “Paramita Wisdom’ Password authentication scheme without verification tables,” *The Journal of Systems and Software*, vol. 42, pp. 45-57, 1998. Article (CrossRef Link)

[8] P. Guo, J. Wang, B. Li, and S.Y. Lee, “A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks,” *Journal of Internet Technology*, vol. 15, no. 6, pp. 929-936, 2014. Article (CrossRef Link)

[9] M.S. Hwang, and L.H. Li, “A New Remote User Authentication Scheme Using Smart Cards,” *IEEE Transactions on Consumer Electronics*, vol. 46, no.1, pp. 28–30, 2000. Article (CrossRef Link)

[10] X Li, J Niu, S Kumari, J Liao, and W Liang, “An enhancement of a smart card authentication scheme for multi-server architecture,” *Wireless Personal Communications*, vol. 80, no 1, pp. 175-192, 2015. Article (CrossRef Link)

[11] X. Li, J. Niu, M. K. Khan, J. Liao, and X. Zhao, “Robust three-factor remote user authentication scheme with key agreement for multimedia systems,” *Security and Communication Networks*, 2014. Article (CrossRef Link)

[12] M.S. Hwang, C.C. Lee, and Y.L. Tang, “A simple remote user authentication scheme,” *Mathematical & Computer Modelling*, vol. 36, pp. 103-107, 2002. Article (CrossRef Link)

[13] C.C. Lee, and M.S. Hwang, and W.P. Yang, “Flexible remote user authentication scheme using smart cards,” *ACM Operating Systems Review*, vol. 36, pp. 46-52, 2002. Article (CrossRef Link)

[14] M.L. Das, A. Saxena, and V.P. Gulati, “A dynamic ID-based remote user authentication scheme,” *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, 629-631, 2004. Article (CrossRef Link)

[15] A.K. Awasthi, “Comment on a dynamic id-based remote user authentication scheme,” arXiv preprint cs/0410011, 2004.

[16] H.Y. Chien, and C.H. Chen, “A remote password authentication preserving user anonymity,” in *Proc. of 19th International Conference on Advanced Information Networking and Applications (AINA’05)*, 2, 245-248, 2005. Article (CrossRef Link)

[17] W.C. Ku, and S.T. Chang, "Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards," *IEICE Transactions on Communication*, vol. E88-B, no. 5, pp. 2165-2167, 2005. Article (CrossRef Link)

[18] W. Shi and D. He, "A security enhanced mutual authentication scheme based on nonce and smart cards," *Journal of the Chinese Institute of Engineers*, vol. 37, no. 8, pp.1090-1095, 2014. Article (CrossRef Link)

[19] T.T. Truong, M.T. Tran, and A.D. Duong, "Enhanced dynamic authentication scheme (EDAS)," *Information System Frontiers*, vol. 16, no. 1, pp. 113-127, 2014. Article (CrossRef Link)

[20] Y.C. Lee, "A new dynamic id-based user authentication scheme to resist smart card theft attack," *Applied Mathematics and Information Sciences*, vol. 6, pp. 355-361, 2012.

[21] B.L. Chen, W.C. Kuo, and L.C. Wuu, "Robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 27, no. 2, pp. 377-389, 2014. Article (CrossRef Link)

[22] F. Wen, D. Guo, and X. Li, "Cryptanalysis of a new dynamic id-based user authentication scheme to resist smart-card-theft attack," *Applied Mathematics and Information Sciences*, vol. 8, no. 4, pp. 1855-1858, 2014. Article (CrossRef Link)

[23] T.T. Truong, and M.T. Tran and A.D. Duong "Modified dynamic ID-based user authentication scheme resisting smart-card-theft attack," *Applied Mathematics and Information Sciences*, vol. 8, no.3, pp. 967-976, 2014. Article (CrossRef Link)

[24] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. of Advances in Cryptology* (*CRYPTO'99*), 388-397, 1999. Article (CrossRef Link)

[25] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, 2002. Article (CrossRef Link)

[26] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987. Article (CrossRef Link)

[27] D. Hankerson, A. Menezes, and S. Vanstone, "*Guide to elliptic curve cryptography*," *LNCS, Springer: New York*, 2004. Article (CrossRef Link)

[28] M.K. Khan, S.K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, 305-309, 2010. Article (CrossRef Link)

[29] S. Kumari, and M.K. Khan, "More secure smart card based remote user password authentication scheme with user anonymity," *Security and Communication Networks*, 2013. Article (CrossRef Link)

[30] D. He, N. Kumar, H. Shen, and J.H. Lee, "One-to-many authentication for access control in mobile pay-TV systems," *Science China-Information Sciences*, vol. 59, no. 5, pp. 1-14, 2016. Article (CrossRef Link)

[31] S. Kumari, and M.K. Khan, "Cryptanalysis and improvement of 'A robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 3939-3955, 2012. Article (CrossRef Link)

[32] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp.263-277, 2015. Article (CrossRef Link)

[33] D. He, and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," *IEEE Systems Journal*, vol. 9, no. 3, pp.816-823, 2015. Article (CrossRef Link)

[34] D. He, S Zeadally, N Kumar, and J.H. Lee, “Anonymous authentication for wireless body area networks with provable security,” *IEEE Systems Journal*, 2016. Article (CrossRef Link)

[35] X. Li, J. Niu, J. Liao, and W. Liang, “Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update,” *International Journal of Communication Systems*, vol. 28, no.2, pp.374-382, 2015. Article (CrossRef Link)

[36] S. Kumari, M.K. Gupta, and M. Kumar, “Cryptanalysis and security enhancement of chen et al.’s remote user authentication scheme using smart card,” *Central European Journal of Computer Science*, vol. 2, no. 1, pp. 60-75, 2012. Article (CrossRef Link)

[37] S. Kumari, M.K. Gupta, M.K. Khan, and X. Li, “An improved timestamp-based password authentication scheme: comments, cryptanalysis and improvement,” *Security and Communication Networks*, vol.7, no.11, 1921-1932, 2014. Article (CrossRef Link)

[38] D. Wang, and P. Wang, “On the Anonymity of Two-Factor Authentication Schemes for Wireless Sensor Networks: Attacks, Principle and Solutions,” *Computer Networks*, vol. 73, pp. 41-57, 2014. Article (CrossRef Link)

[39] D. Wang, Q. Gu, H. Cheng and P. Wang, “The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes,” in *Proc. of the 11th ACM Asia Conference on Computer and Communications Security (AISACCS 2016)*, pp. 475-486. Article (CrossRef Link)

[40] K.M. Martin, “Everyday cryptography: Fundamental principles and applications,” Oxford University Press, Chapter 13, p. 495, 2012. Article (CrossRef Link)

[41] L. Zhang, S. Tang, and S. Zhu, “An energy efficient authenticated key agreement protocol for SIP-based green VoIP Networks,” *Journal of Network and Computer Applications*, vol.59, pp. 126-133, 2016. Article (CrossRef Link)

[42] Q. Jiang, J. Ma, G. Li, and X. Li. “Improvement of robust smart-card-based password authentication scheme,” *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383-393, 2015. Article (CrossRef Link)

[43] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He., “A privacy preserving three-factor authentication protocol for e-health clouds,” *Journal of Supercomputing*, 2016. Article (CrossRef Link)

[44] R. Canetti, and H. Krawczyk, “Analysis of key exchange schemes and their use for building secure channels,” in *Proc. of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology-Eurocrypt* 2001, pp. 453-473, 2001. Article (CrossRef Link)

[45] D. Wang, D. He, P. Wang, and C. Chu, “Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment,” *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 228-44, 2015. Article (CrossRef Link)

[46] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” *ACM Transactions on Computer System*, vol. 8, pp. 18-36, 1990. Article (CrossRef Link)

Dr. Saru Kumari is currently an Assistant Professor with the Department of Mathematics, C.C.S. University, Meerut, U.P, India. She received Ph.D. degree in Mathematics in 2012 from C.C.S. University, Meerut, Uttar Pradesh, India. She has published 45 papers in international journals and conferences including 30 research publications in SCI indexed journals. Her current research interests include Information Security, Digital Authentication and Security of Wireless Sensor Networks.

Dr. Xiong Li is currently an Associate Professor at School of Computer Science and Engineering of the Hunan University of Science and Technology (HNUST), China. He received Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications (BUPT), China in 2012. He has published more than 45 referred journal papers in his research interests, which include cryptography and information security, etc. He is a winner of the 2015 Journal of Network and Computer Applications Best Research Paper Award.

Mr. Fan Wu received the Bachelor degree in Computer Science from Shandong University, Jinan, China in 2003, and received Master degree in Computer Software and Theory from Xiamen University, Xiamen, China in 2008. Now he is a lecturer in Xiamen Institute of Technology, Huaqiao University. His current research interests include information security, internet protocols, and network management.

Dr. Ashok Kumar Das received the Ph.D. degree in Computer Science and Engineering, the M.Tech. degree in Computer Science and Data Processing, and the M.Sc. degree in Mathematics, all from IIT Kharagpur, India. He is currently an Assistant Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He has authored over 80 papers in international journals and conferences in his research areas. His current research interests include cryptography, wireless sensor network security and proxy signature.

Mr. Vanga Odelu received the M.Tech. degree in computer science and data processing from IIT Kharagpur, India, in 2011, where he is currently pursuing the Ph.D. degree with the Department of Mathematics. He has authored 18 papers in international journals and conferences. His research interests include cryptography, network security, and hierarchical access control.

Dr. Muhammad Khurram Khan is currently a Professor with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He has edited seven books and proceedings published by Springer-Verlag and IEEE. He has published more than 145 papers in international journals and conferences and he is an inventor of 7 U.S./PCT patents in the information security field. He is on the editorial boards of several International SCI journals Dr. Khurram is one of the organizing chairs of several top-class international conferences and he is also on the program committee of dozens of conferences. His current research interests include biometrics, multimedia security, and digital authentication. He is a senior member of the IEEE and a member of the IEEE Consumer Electronics society.